معلومات أمنيّة

غير مشفّرة



سيف محمد الكعبي

حول الكتاب

هذا كتاب توعوي حول أمن المعلومات ، بإمكان الجميع قرائته لأنّ اللغة المستخدمة مبسّطة ، بعد قراءة الكتاب ستصبح أكثر حمايتاّ وأقل تعرضاَ للاختراق ، وسيصبح لديك حسّ أمني الكتروني ، فالإحساس الخاطئ بالأمن أخطر من الإحساس الصحيح بعدم الأمن.

سيف محمد الكعبي

معلومات أمنيّة غير مشفّرة

UNENCRYPTED SECURITY INFORMATION

SAIF MOHAMMED AL KAABI

UNENCRYPTED SECURITY INFORMATION



SAIF MOHAMMED AL KAABI

ABOUT THE BOOK

This is an awareness book about security information, it's available for everyone and readable because the language of the book is very simple. After reading this book you will become more protected and less exposed from hackers, and you will have a digital sense of secure. The wrong feeling of security is more dangerous than the correct feeling of insecurity

معلومات أمنيّة
غير مشفرة

معلومات أمنيّة
غير مشفرة

سيف محمد الكعبي

الطبعة الأولى
2018م



المملكة الأردنية الهاشمية

رقم الإيداع لدى دائرة المكتبة الوطنية

(2018/7/3145)

Isbn 978-9957-99-882-0



أصبحت المعلومات الأمنية ذات أهمية كبيرة في العديد من المؤسسات وتؤثر عليهم في العديد من الجهات. في هذا الكتاب، سوف يزيد سيف الكعبي من أهمية الوعي الأمني المعلوماتي وعرض التأثيرات من خلال الاهتمام بالخصوصية والتحديات التي جلبها الأمن المعلوماتي لعالمنا اليوم وزيادة التعريف عن المخاطر التي تواجه الأمن المعلوماتي. ويضيف الكتاب أيضاً مفهوم النقاط الرئيسية لأمن المعلومات وفوائد التكنولوجيا التي تتعامل مع العديد من قضايا وتحديات المعلومات الأمنية.

الدكتور خالد سمارة

رئيس قسم - تكنولوجيا الكمبيوتر والمعلومات

كلية العين للطلاب

لقد رأيت سيفًا يستكشف الحلول الأمنية الإلكترونية المتطورة منذ لقائي به، كان يشغل العديد من حملات التوعية الأمنية في المجتمع، وخاصة للطلاب الصغار الذين يستخدمون الأجهزة الذكية للاستخدام الخاص. حملات التوعية مفيدة للغاية للمجتمع، وذلك للحفاظ على الحماية ضد الهجمات الخبيثة. الكتاب يجب أن يقرأ للجميع وعلى وجه التحديد لمستخدمي الهواتف الذكية الذين يستخدمونها للاستخدام الخاص.

الدكتور منير نافيد

أستاذ مساعد - علوم الكمبيوتر والمعلومات

كلية العين للطلاب

الأمن السيبراني من أهم التخصصات والمهارات، والطلب عليه في ازدياد، وذلك منذ عام 2005 ولغاية الآن ومستقبلاً نظراً لارتفاع استخدام التقنية وازدياد فرص وامكانية تسريب وسرقة البيانات وانتهاك الخصوصية لكل المستخدمين والاجهزة من جوالات، تلفزيون ذكي، سيارات ذكية، أجهزة منزلية ذكية حتى انتشار البرامج الضارة والحرب الالكترونية ضد الجهات الحكومية والشركات مما تسبب في خسارة مئات الملايين من البيانات والأموال.

ومن المهم تهيئة كوادر وطنية وعربية و وضع خطط لصد وتفادي المخاطر السيبرانية وحماية خصوصيتنا، وفي دراسة أنه في عام 2021 ستتوافر ما يقارب 3.5 مليون وظيفة سيبرانية، ونحن بحاجة لمحترفين ومتخصصين في هذا المجال، لكن في الشرق الأوسط لازال هناك ضعف وافتقار للمهنيين والمحترفين في هذا المجال بشكل تطبيقي عملي وايضاً ضعف في المصادر العربية لتثقيف الأمة العربية من الشباب ولكن بمثل هذا الكتاب العربي وبعض مبادرات الشباب العربي مؤخراً لرفع مستوى الثقافة الأمنية نفخر وبالتأكيد سيكون بصمة مشرفة للوطن العربي والإسلامي في مجال الأمن السيبراني.

الدكتور ياسر العصيفير

رائد أعمال في الأمن السيبراني

المقدمة:

انا لست كاتبًا لكنني محب وغيور على وطني الذي علمني الكثير وساعدني على تحقيق أحلامي، بدأت بتوعية المجتمع بمخاطر الإنترنت عن طريق إلقاء المحاضرات واكتشفت بأن مجتمعنا يحتاج إلى الكثير من التوعية الأمنية، وهذا ما حفزني على تأليف كتاب توعوي لجميع فئات المجتمع.

لا شك في أن أمن المعلومات بات أحد القطاعات الأسرع نموًا في هذه الأيام، خصوصًا مع التزايد المستمر للهجمات والجرائم الإلكترونية، فلا تكاد تمر عدة أيام حتى نسمع بعمليات تسريب لبيانات المستخدمين أو عمليات احتيال إلكترونية هنا وهناك، وهو الأمر الذي يستدعي من الشركات التجارية المختلفة إعطاء المزيد من الأولوية للخدمات المتعلقة بالحماية الإلكترونية، ويجب على الدول زيادة الوعي لأفراد المجتمع لكي لا يقعوا ضحايا الجرائم الإلكترونية.

أصبحت حياتنا اليومية مملة، وأصبح التواصل بين الناس للمصالح فقط، صحيح بأن الإنترنت له فوائد عديدة، حيث أصبح التواصل بين الشركات والدول سريعًا، وأصبحت الدوائر الحكومية أكثر نشاطًا، وأصبح المواطن أكثر فعالية، لكن مستقبلًا ستصبح

سلبياته أكثر، ويجب علينا الاستعداد لتصدي السلبيات المتوقعة، فالحرب القادمة هي حرب إلكترونية.

ما التوعية الأمنية؟

التوعية الأمنية: أن يكون كل فرد على علم ودراية بمسؤوليته تجاه حماية المعلومات والأجهزة التي يستخدمها سواء أكانت المعلومات شخصية تابعة لجهة العمل وإدراكه التام لأهمية عدم البوح بكلمات المرور أو المعلومات الأمنية المهمة في الشركة ومعرفته للأخطار المترتبة على أي من التجاوزات الأمنية، وهي تنمية وتعزيز المسؤولية الفردية والفهم الكامل بأهمية تطبيق القواعد الأمنية الموضوعة من قبل الجهات العليا والحرص على عدم تجاوزها.

تعتبر التوعية الأمنية من أهم خطوط الدفاع وحماية المعلومات والموارد لأنها الأقل تكلفة فقد أثبتت الدراسات أن المبالغ التي تنفق على توعية الموظفين أو الناس عموما أقل بكثير من المبالغ التي تصرف على إصلاح الأضرار الناجمة عن تسريب معلومات ووصولها لمتناول أشخاص غير مصرح لهم أو حتى تدميرها وتخريبها.

المستهدفين بالتوعية الأمنية؟

أهم الفئات المستهدفة بالتوعية الأمنية، هم الموظفون في المؤسسات والمنظمات وحتى الحكومات أيضًا، وذلك لتمكنهم الاطلاع على معلومات مهمة وحساسة لا يسمح لأحد غيرهم الاطلاع عليها كلٌ حسب رتبته ومنصبه الإداري وحاجته لهذه المعلومات.

لماذا نحتاج التوعية الأمنية؟

لا يستطيع قسم أمن المعلومات في الشركة تحمل جميع الأخطار ومواجهتها بمفرده، لذلك فإن كل موظف في الشركة يتحمل جزءًا من المسؤولية تجاه الأخطار المحتملة ومحاربتها ومنع وقوعها. فقد يتسبب ضعف الثقافة الأمنية لموظف واحد فقط في تدمير جهة عمل بأكملها، لذا يجب تثقيف الموظفين في جميع جهات العمل من أقل إلى أعلى مرتبة في العمل لضمان وعي عالٍ بأمن المعلومات.

الهندسة الاجتماعية:

لك أن تتخيل أن الهندسة الاجتماعية تحدث كل دقيقتين في الولايات المتحدة الأمريكية، ففي سياق أمن المعلومات والأمن الرقمي،الهندسة الاجتماعية هي القدرة على الحصول على معلومات حساسة وسرية عن طريق التلاعب بعقول الأشخاص بأساليب انتحال الشخصية أو الحصول على ثقة الضحية بشكل تدريجي، بمعنى أنها تساعد على اختراق الأنظمة من خلال التلاعب بالبشر وليس من خلال التلاعب بالآلات. الهندسة الاجتماعية من أقصر وأبسط الطرق لاختراق الأنظمة حتى إنها تشكل المدخل لأكثر من 70 % من الاختراقات التي تحدث في العالم، فهي لا تعتمد على معرفة تقنية عميقة بالتالي يستطيع أي شخص يتوافر لديه قدر معين من الحنكة والدهاء القيام بهجمات الهندسة الاجتماعية. ولتجنب الوقوع ضحية هذا النوع من الهجمات،احرص على خصوصيتك وعدم نشر معلومات شخصية عن نفسك لأن المهاجم قد يستخدمها لانتحال شخصيتك، ولا تثق بأحد، وانظر بعين الحذر إلى كل بريد إلكتروني أو رسالة تصلك تحتوي على ملفات وروابط مرفقة.

تخيل أن اختراق الكاميرا يستغرق من المخترق جزءًا من الثانية، ويمكن ابتزازك إلكترونيًّا مدى العمر، فاحرص على وضع شريط لاصق على الكاميرا لتجنب ذلك

تعريف أمن المعلومات:

أمن المعلومات هي مجموعة من السياسات والإجراءات الفنية المتخذة من أجل منع الأشخاص غير المخولين من الدخول إلى الشبكات وتغيير معلوماتها، سرقتها أو تدمير نظم المعلومات. لكن من وجهة نظري أن أمن المعلومات هو عملية الحفاظ على المعلومات بشكل آمن، وحمايتها من الوصول غير المصرَّح به. وذلك لكي تبقى محمية و آمنة. في أمن المعلومات يوجد ثلاثة أسس رئيسة:

- **السرية:**

السرية تعني التأكد من أن المعلومات لا تكشف ولا يمكن أن يطلع عليها من قبل اشخاص غير مخولين بذلك.مثال: مستند لا يحق لأي موظف الاطلاع عليه إلا المدير.

- **التكاملية:**

التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو العبث به وبشكل خاص لن يتم تدمير المحتوى أو تغيره أو العبث به في أية مرحلة من مراحل المعالجة أو التبادل سواء أكان في مرحلة التعامل الداخلي مع المعلومات أو عن طريق تدخل غير مشروع. مثال: تعميم لا يحق لأي شخص التعديل عليه.

- **توافر المعلومات او الخدمة :**

التأكد من استمرار عمل النظام المعلوماتي واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية وأن مستخدم المعلومات لن يتعرض إلى منع استخدامه لها أو دخوله إليها.مثال: إمكانية الدخول إلى صفحة النظام الخاصة بالموظفين.

لماذا أمن المعلومات مهم ؟

أمن المعلومات مهم جدًا مع تقدم التكنولوجيا، فأصبح الاعتماد على أنظمة المعلومات في إنجاز العمل بشكل كبير، إضافةً لانتشار استخدام شبكات الحاسب والإنترنت، ولا ننسى أن تطور مجال التقنية المعلوماتية أصبح سريعا،وهذا لوحده يُعدّ خطرًا، لأننا لسنا مستعدين لهذا التطور السريع، لماذا ؟ لأننا لا نملك أدوات لحماية معلوماتنا، ولا يوجد مستثمرين ومطورين مهتمين ببرامج الحماية !، وبهذا التطور السريع وإهمال الأمن الإلكتروني نكون قد فتحنا باب الاختراق للمخترقين.

فوضى وسائل التواصل الاجتماعي:

هذه هي حياتنا اليومية لا تخلو من وسائل التواصل الاجتماعي التي لا يستغلها الناس إلا لمصالحهم الشخصية، فكل من دخل هذا المجال أصبح مشهورًا، وأصبحت المسألة معكوسة، فمن المتعارف عليه أنه كلما زاد الطلب زاد العرض، ولكن بوجود وسائل التواصل الاجتماعي انعكست الجملة وأصبحت "كلما زاد العرض زاد الطلب"!، وأصبح الجميع مثقفًا فجأة، فمثلا لو دخلت تويتر ستجد شخصًا يكتب عن كل شيء، وإذا دخلت السناب شات فستجد شخصًا يتكلم في كل شيء، وهذا هو الحال في باقي الوسائل .

هذه البرامج أسست لأهداف عدّة لكن أغلبها لا يناسب المستخدمين، فتطرقوا لوضع أهداف تناسبهم، إذا وضعت رأيك الخاص ولم يعجبهم فستتلقى الشتائم بأنواعها، وإذا شاركت بصورة أيضًا ولم تعجبهم ستلقى سيلًا من الشتائم، الحياة لم تتغير والناس لم يتغيروا لكن المبادئ والقيم هي التي تغيرت. فجملة قل خيرًا أو اصمت لم تعد موجودة في قاموس حياتنا اليومية.

أصبحت الحروب كلامية إلكترونية، فإذا ما حدثت أزمة في دولة ما لا تفتح الأخبار لتتطلع عليها، فقط افتح أحد وسائل التواصل الاجتماعي وسترى العجب العجاب، سترى هجومًا بين

المؤيدين والمعارضين، وسترى أبناء الدولة الواحدة يتبادلون الشتائم، أليست الأزمة في دولتكم؟! ألستم شعبًا واحدًا!. نحن في دوله الإمارات العربية المتحدة تعلمنا من قائدنا وقدوتنا المرحوم الشيخ زايد بن سلطان آل نهيان رحمه الله، أنه مهما حصل نبقى مع الإمارات وقادتها وليس ضدها، ونكون يدا واحدة، أسس فينا الوحدة الوطنية وحب الوطن، فتدمع عيناي إذا رأيت شخصا يشتم الإمارات، فالإمارات خطٌّ أحمر.

أحد طرق الاختراق باستخدام الرسائل النصية وهي إرسال روابط وهمية في رسائل نصية مثل: ربحت كوبون شراء، ربحت مبلغًا ماليًّا، حدِّث بياناتك، سجل لدخول السحب، صورتك في الرابط، وغيرها من الخدع! تتم سرقة المعلومات أو التعرف على جهازك ومكانك.

كيف تحمي أبناءك من مخاطر الإنترنت؟

تذكر دائمًا بأن وعيك هو سبيل أمنك وأمن أبنائك، فيجب عليك تحذيرهم من مشاركة المعلومات الشخصية مع الغرباء أيًّا كانوا، واحرص على أنهم يأخذون الإذن المسبق منك في حال رغبتهم في مشاركة البيانات، وإضافة إلى ذلك تابع نوعية البيانات التي تنشر من قبلهم على شبكات التواصل الاجتماعي، فالإنترنت مليء بالغرباء هدفهم دائمًا إلحاق الضرر لمن لا يملكون توعية أمنية، سواء بالابتزاز أو سرقة المعلومات الشخصية، فأطفالنا لا يفقهون شيئًا، ومن واجبنا تثقيفهم وإرشادهم بكيفية تحقيق الأمن الإلكتروني.

بعض أنواع البرامج التي تشكل تهديدًا لنظم المعلومات:

الفيروسات الحاسوبية:

هي عبارة عن برامج حاسوبية والتي ترتبط ببرامج حاسوبية أخرى أو ملفات بيانات من أجل تنفيذها بطريقة خاطئة.

البرامج الدودية worm:

هي برامج حاسوبية مستقلة تقوم بنسخ نفسها من كمبيوتر إلى آخر عبر الشبكة.

برنامج حصان طروادة trojan horse:

هو برنامج في ظاهره يبدو أنه سينفذ شيئًا معينًا ولكن عند البدء يقوم بعمل آخر مضر بنظم المعلومات.

هجمات الحرمان من الخدمة :(Denial of Service Attacks)

وتعرف أيضًا بهجوم حجب الخدمة، وهي عبارة عن هجوم يشنّه قرصان عابث إلكترونيًّا بإمداد عدد من المواقع بكميّاتٍ هائلة من البيانات غير الضرورية، وتكون محمّلةً بالبرامج الخبيثة التي تنشر داءها فور وصولها إلى الجهاز، فتبدأ بالدمار الذي يؤدّي في بداية الأمر إلى تراجع مستوى الخدمة الخاصة بالاتصال بالإنترنت، ويُسبّب صعوبةً في الوصول إلى الخدمات نظرًا لضخامة البيانات المرسلة إلى الجهاز.

برامج التجسس Spyware :

هي برامج حاسوبية تقوم بالنزول بشكل سريٍّ عبر الشبكة وتقوم بتسجيل الكبسات التي استخدمت من أجل معرفة الكلمات السرية والأرقام المتسلسلة.

الجامع المشترك بين هذه البرمجيات انها برمجيات ضارة تستغل للتدمير سواء تدمير النظام او البرمجيات او المعطيات أو الملفات أو الوظائف أو تستثمر للقيام بمهام غير مشروعة كإنجاز احتيال أو غش في النظام، والحقيقة انها ليست تسميات مترادفة للفيروسات الشائعة، إنها تختلف عن بعضها بعضًا من حيث تركيبها احيانا واحيانا من حيث طريقة إحداث النتيجة وأحيانا أسلوبها في الهجوم.

التشفير:

تحظى تقنيات وسياسات التشفير في الوقت الحاضر باهتمام استثنائي في ميدان أمن المعلومات، وسبب ذلك أن حماية التشفير تمثل الوسيلة الأكثر أهمية لتحقيق وظائف الأمن الثلاثة، السرية والتكاملية وتوفير المعلومات، وهو مكون رئيس لتقنيات ووسائل الأمن الأخرى، خاصة في بيئة الاعمال الإلكترونية والتجارة الإلكترونية والرسائل الإلكترونية وعموما البيانات المتبادلة بالوسائط الإلكترونية.

ومن حيث مفهومه، فإن التشفير يمر بمرحلتين رئيستين، الأولى تشفير النص على نحو يحوله إلى رموز غير مفهومة، والثانية، فك الترميز بإعادة النص المشفر إلى وضعه السابق كنص مفهوم ومقروء، وهذه المسألة تقوم بها برمجيات التشفير التي تختلف أنواعها ووظائفها.

تزويد الشخص بوسائل الحماية من الاختراق يوفر له حماية لفترة قصيرة، ولكن تعليمه كيف يدقّق هذه الوسائل يضمن له حماية أطول.

حرب المعلومات:

الحرب العالمية الثانية هي ليست آخر الحروب، فهناك حروب معلوماتية حدثت وأنا أعني الحرب، وليست مجرد الاختراق أو التخريب أو التنصت، تستخدم المعلومات وتقنية المعلومات كأسلحة، تكون على مستوى واسع و ضد أهداف معلوماتية، تحدث عند الرغبة وليس عند القدرة. حرب المعلومات قد تتضمن جمع المعلومات الاستراتيجية، التأكد من صلاحية المعلومات الموجودة، نشر دعايات أو معلومات خاطئة لإحباط العدو أو الشعب، التقليل من نوعية المعلومات التي توجد لدى العدو والعمل على تقليل فرص جمع العدو للمعلومات. وقد أصبحت الحرب الإلكترونية المعلوماتية جزءًا مهما من الحرب العسكرية، ولعل كلام رئيس جهاز الاستخبارات الألمانية أوغست هانينغ مازال ماثلًا حين قال "إن الحروب ستدور من الآن فصاعدا في مجال المعلوماتية وخصوصا الإنترنت، وإن الجيوش تدرب الجنود على القرصنة المعلوماتية، وكل دولة تقوم بإعداد فيروسات لشل الاتصالات والمعلومات في جبهات العدو".

ما الحلقة الأضعف في أي نظام؟

مهما كان النظام آمنًا وعليه درجات أمان عديدة فهذا لايعني أنه لا يمكن اختراقه، لأنه لا يوجد نظام آمن 100%، ولو فرضنا أن النظام مؤمن بشكل جيد من برامج حماية، أين تكمن الحلقة الأضعف فيه؟

الإنسان، نعم الإنسان أو المستخدم هو أضعف حلقة في النظام فأغلب الهجمات التي تحدث الآن تعتمد على أخطاء الإنسان (يضغط على رابط مشبوه، يفتح ملفًا فيه فايروس، يرد على إيميل تصّيد..... إلخ).

أهم أسباب الإصابة بفايروس:

٤٦٪ إيميلات التصيّد*(Phishing Emails) .

٣٦٪ افتقاد الموظفين للتدريب الجيد.

٢٣٪ المواقع والإعلانات المشبوهة.

١٪ ضعف في النظام الأمني.

٥٪ أسباب اخرى.

التقنية من صنع البشر وهم الشريك الأساسي في بنائها، وهم من يتحمل كامل المسؤولية عن وقوع الأخطاء، فالخطأ البشري وارد لكن اكتشافه يتطلب الكثير من الجهد والوقت، ولا ننسى بأن هناك إمكانية بالتأثير النفسي عليهم وخداعهم، وأيضا هناك إهمال من قبل البشر في تطبيق التعليمات الأمنية إما عمدًا أو نسيانًا أو تجاهلًا، والتقنية تتطور يومًا بعد يوم بتسارع ملحوظ مما يتطلب المتابعة المستمرة وتحديث المعلومات الشخصية.

---

*إيميلات التصيّد:

هو باختصار التزوير أو خداع الشخص(جزاء من الهندسة الاجتماعية) ، بمعنى أصح أن يقوم احد بعمل موقع يشابه موقعًا تجاريًا 100%

ما قانون حماية البيانات الجديد من الاتحاد الأوربي ؟

لاحظنا في الآونة الأخيرة وصول العديد من الرسائل على البريد الإلكتروني من شركات عالمية يبلغوننا بأنهم حدثّوا شروط الاستخدام!، سبب حالة الاستنفار العالمية هذه هو أن الاتحاد الأوربي بدأ بتطبيق قانون حماية خصوصية المعلومات الجديد.

٢٥مايو ٢٠١٨طبّق هذا القانون على جميع الشركات التي تتعامل مع بيانات الأفراد سواء في أوربا (أو خارج أوربا ولهم تحكم على معلومات أفراد بأوروبا)، القانون مهتم جدًا بأن تكون معلومات الناس في أمان، وأن يكون لدى المستخدم تحكم كامل على معلوماته. أتمنى أن نجد مثل هذه القوانين في دول العالم أجمع وليس في دول الاتحاد الأوربي فقط.

تقسيم الإنترنت

هل سمعت بما يسمى بالإنترنت المظلم أو العميق وأن شبكة الإنترنت نفسها تنقسم إلى عدة شبكات ، حيث يمكن تقسيم الإنترنت إلى ثلاثة أقسام:

- الإنترنت الظاهري.
- الإنترنت العميق.
- الإنترنت المظلم.

الإنترنت الظاهري:

الإنترنت الظاهري هي شبكة الإنترنت التي نستخدمها يوميا كالبحث في غوغل أو مشاهدة المواضيع، و هي مجموعة المواقع التي تصل إليها محركات البحث و تقوم بفهرستها و يمكننا الوصول إليها عن طريق محركات البحث أو مباشرة عن طريق روابطها حيث إنها لا تمثل أكثر من 4% من شبكة الإنترنت.

الإنترنت العميق:

الإنترنت العميق أو الإنترنت السفلي هي أكبر قسم من شبكة الإنترنت حيث تمثل مجموعة المواقع و البيانات التي لا تصل إليها محركات البحث ولا تقوم بفهرستها لكن نستطيع الوصول إليها مباشرة بطرق خاصة كأداء بحث الاستعلام الداخلي ، مثل خدمات البريد الإلكتروني و معلومات البنوك و رسائل الفيسبوك فهي معلومات لا يمكن لمحركات البحث الوصول إليها لكن نستطيع الوصول إليها مباشرة فهي ضمان للحفاظ على خصوصية المستخدمين و هو يمثل تقريبا 94% من محتوى الإنترنت.

الإنترنت المظلم:

الإنترنت المظلم هو عبارة عن مجموعة المواقع و البيانات التي لا تقوم محركات البحث بأرشفتها و لا يمكننا الوصول إليها مباشرة ، حيث إنها تحتاج إلى أدوات أو إعدادات خاصة تمكننا من تصفح مواقعها ، مثل شبكة تور. تختلف استخدامات الإنترنت المظلم من شخص لآخر لكن كونه بعيدا عن أي مراقبة فهو يعتبر مركزاً لكل ما هو غير قانوني فهو أنسب مكان لعالم الجرائم و المخدرات، حيث توجد مواقع لبيع المواد المحظورة كبيع الأسلحة و القنابل و بيع المخدرات و مواقع أخرى تقوم بتعليم الاختراق و بيع الثغرات البرمجية و الهويات و بيع الجنسيات العالمية و أخرى تقدم وثائق مزورة و تجد غيرها من المواقع غير القانونية ، و يتم استخدام عملات افتراضية في التعامل في هذا الفضاء كعملة **البتكوين**.

عملة البِتْكويْن:

في عام 2009 قام شخص مجهول بنشر بحث على الإنترنت يشرح فيه العملة الإلكترونية، وكيف تعمل وما شروطها بطريقة دقيقة ومعقدة وسماها البتكوين، من بعدها العالم بدأ في التعرف على هذه العملة والتعامل معها والوثوق بها، وهي عملة الكترونية تعتمد على التشفير بشكل أساسي،وبات الوصف المم‍ل لـ "بتكوين" بأنها عملة رقمية لا وجود فيزيائي لها، يزيد من الغموض الذي تستمده هذه الأداة أو العملة، من غموض مبتكرها، وغموض مصدر إدارة الشبكة المحمية التي توفرها عبر الإنترنت بمختلف دول العالم، ومن مميزات العملة الإلكترونية أنها ترسل من شخص لشخص لا تحتاج الى وسيط في النقل، لذلك يفضلها المخترقون عند طلب الفدية، وقد يصل سعر العملة الواحدة الى 27500 درهم إماراتي، فقيمتها تتزايد بزيادة الإقبال عليها.

عند الافراط في السماح للتطبيقات غير المعروفة في معرفة (موقعك، ألبوم الصور، الكاميرا، المايكروفون) فأنت تعرض نفسك لانتهاك الخصوصية لأنها ستستمر في معرفة معلوماتك بشكل مستمر ودون إذنك.

إدوارد سنودن:

كيف لي أن أكتب عن أمن المعلومات ولا أذكر إدوارد سنودن، إدوارد سنودن هو من مثّل شخصية البطل في مسلسل أمن المعلومات، هو خبير كمبيوترات محترف أميركي الأصل، وعميلٌ سابق للدولة الأميركية، وهو الذي قام بنشر فضائح حول العديد من العملاء الذين صنفهم غير أخلاقيين. وكان السبب هو أن ممارساتهم مزعجة ولا تعبر عن دستور الولايات المتحدة، وأعتقد أن فضحهم هو الشيء الصحيح الذي يجب القيام به لإطلاع العالم على ما كانت عليه وكالة الأمن القومي، وكشف تورط وكالة الأمن القومي في بعض ممارسات المراقبة المحلية، التي كان يعتقد أنها تنتهك الخصوصية وقضى عدة سنوات في جمع الأدلة حتى فضحهم واتهمهم أمام الملأ وفي مؤتمر صحفي في هونج كونج بانتهاك خصوصية الناس. من خلال البيانات قال فيه: إن وكالة الأمن القومي يمكنها الحصول عليها تتضمن: رسائل البريد الإلكتروني، ومحادثات الفيديو والصوت، والصور، والاتصالات الصوتية برتوكول الإنترنت، وعمليات نقل الملفات، وإخطارات الولوج وتفاصيل الشبكات الاجتماعية.

دول العيون الخمسة:

تتعاون دول "العيون الخمسة " وهي الولايات المتحدة الأمريكية، المملكة المتحدة، كندا، إستراليا ونيوزيلندا فيما بينها في مجال التجسس والمراقبة والتسلل لشبكات الدول ومراقبة الاتصالات وتتولى قيادة هذا التحالف وكالة الأمن القومي ومركز الاتصالات البريطاني وقد غردت كثيرًا عنهم قبل سنوات عندما نُشرت تسريبات إدوارد سنودن!، لك أن تتخيل أن جميع ما نكتبه أو نرسله عبر الإنترنت مراقب من قبل دول العيون الخمسة، فهذا التعاون بين الدول سبب العديد من المشاكل، وأهمها انتهاك الخصوصية، فالخصوصية حق لكل إنسان في الكرة الأرضية.

الخصوصية و الأمان:

هل مفهوم الخصوصية و الأمان واحد ؟ طبعا لا، الأمان يعني كمستخدم أنه يجب أن أشعر بالأمان بشكل عام، وبشكل خاص أن يتوافر لي أجهزه وبرامج آمنة. أما الخصوصية فتعني كمستخدم أن أشعر بالخصوصية عند استخدام البرامج والأجهزة ولا يوجد أحد يراقبني أو يستعمل معلوماتي الشخصية. لكن مع دخول التقنية بشكل كبير لحياتنا فمن الصعب علينا أن نتحكم هل نسمح لهم أم لا بالتدخل بخصوصياتنا، لكن من الممكن أن نتحكم بنوع وكمية المعلومات التي نعطيها للتقنية عن حياتنا، ودائمًا هناك مقولتان تتكرر : لكي أحميك يجب علي مراقبتك، إذا لم ترتكب خطأ فلماذا تخاف من المراقبة ؟، طبعاً أنا لا أتفق مع المقولتين لكن فيهما القليل من الصحّة، المفروض أن المقولتين يكمّل بعضهم بعضًا إذا تم استعمالهما بطريقة متساوية، لكن الواقع أن بينهم علاقة طردية، فاذا طلبت الأمان فهذا سيؤثر على خصوصيتك.

الذكاء الاصطناعي:

علم الذكاء الاصطناعي أحد أهم العلوم الداعمة للأمن الإلكتروني، علم ذو مستقبل واعد، فالذكاء الاصطناعي هو قدرة الآلة على محاكاة العقل البشري كقدرته على التفكير والاكتشاف والاستفادة من التجارب السابقة، بمعنى آخر أن الأجهزة الإلكترونية ستصبح ذكية تفهم ما يريده الإنسان، وسيصبح لها فائدة أكبر، فتقنيات الذكاء الاصطناعيّ تُعدّ الآن منتشرة في كل جزء من أنحاء العالم، ولهذا السبب هي لا تُعدّ ولا تحصى، وأفضل مثال على الذكاء الاصطناعي هو الروبوت، فالمتوقع مستقبلًا بأن الروبوت سيقوم بمهام الإنسان، وأيضًا قادر على توفير الأمن الإلكتروني وتخفيف مخاطر الإنترنت،فهو استشراف للمستقبل وللأمن الإلكتروني، كانت تقنيات الذكاء الاصطناعي في البدء مجالًا للباحثين في الجامعات، إلا أنه يتزايد حاليًّا لجوء شركات التكنولوجيا إليها لمتابعة سلوكيات مستخدميها على الإنترنت، والتنبؤ بخطواتهم التالية، وبالمثل تستعين بها شركات أمن المعلومات لمواجهة التصاعد المُتواصل في حوادث الاختراق، ومواجهة القراصنة باستراتيجيات تُشابه أساليبهم، فيسعدني كثيرًا وجود وزير للذكاء الاصطناعي في دولتي الحبيبة الإمارات، علمًا أن حكومة دولة الإمارات ستوفر مع الذكاء الاصطناعي 50% من التكاليف السنوية.

مخاطر الجيلبريك، برامج البلس، والبرامج من خارج المتاجر والمواقع الرسمية، بمجرد تثبيتك لها فأنت تعرض هاتفك للاختراق وبياناتك للسرقة ومنها سرقة الصور والفيديوهات الخاصة، قوائم المحادثات والأرقام والملفات كل هذا وأكثر دون علمك.

إنترنت الأشياء:

كثيرة هي الجهات التي حاولت وضع تعريف دقيق لإنترنت الأشياء و ذلك لعدم وجود جهة تمتلك أو تتحكم بإنترنت الأشياء فبالتأكيد لن يكون هناك تعريف رسمي، و لكن ببساطة جميع التعاريف تصب في مفهوم واحد و الذي أحب أن أوضحه بالنص الآتي:

"إنترنت الأشياء هو مفهوم متطور لشبكة الإنترنت، بحيث تصبح كل الأشياء في حياتنا قابلة بالاتصال بالإنترنت أو ببعضها بعضًا لإرسال و استقبال البيانات لأداء وظائف محددة من خلال الشبكة."

لا تحب التعريفات النظرية؟ أنا كذلك ببساطة إنترنت الأشياء هو العالم الذي بدأنا نعيش بعضًا من جوانبه حاليًا حيث إن بعض الأشياء التي نستخدمها أصبحت لديها قدرة الاتصال بالإنترنت، مثلًا الساعات، التلفزيونات، النظارات و غيرها. لكن ما الذي يخفيه لنا هذا العالم غير ما ظهر حتى الآن و ما المقصود بـ "الأشياء" في عبارة إنترنت الأشياء؟

ما "الأشياء" في إنترنت الأشياء ؟:

كل شيء، كل شيء موجود بمعنى الكلمة يدخل تحت مفهوم إنترنت الأشياء مثل: الملابس، الأثاث، الأواني المنزلية، أعضاء الجسم، الشوارع، بل وحتى الحيوانات! أي شيء يمكن أن يلتصق به وحدة معالجة و خاصية اتصال بالإنترنت يعتبر شيئًا في عالم إنترنت الأشياء. يعني ذلك إذا كان هناك خلل في التقنية سيكون هناك خلل في حياتنا، ومن أهم العواقب التي قد تواجهها إنترنت الأشياء هو الأمن ، فإذا أصبحت حياتنا كلها مرتبطة بالإنترنت فكيف سنحميها من المخترقين؟

بالطبع فإن التقنية الأمنية لن تطبق بنسبة 100% إلا بعد توفير الأمن، وسأظل متمسكاً بوجهة نظري أن انترنت الأشياء سيشكل خطرًا على حياتنا إذا طبقت، وذلك لأنه لا يوجد أمن كامل.

فيروس الفدية:

فيروس الفدية من أخطر الفيروسات التي تصيب الأنظمة ويتم تشفير وقفل النظام بالكامل ويطلب المخترق مبلغًا ماديًا مقابل فك قفل الملفات، هذا الفيروس غالبًا يستهدف البيانات الحساسة ووجهات العمل كالشركات والمؤسسات والوزارات والمستشفيات والجامعات. يبدأ هذا الهجوم الإلكتروني مع وصول رسالة أو رابط من شخص مجهول يطلب تحميل الملف على أنه ملف مهم أو شخصي. وفور تحميل الملف في الكمبيوتر أو الهاتف الذكي تبدأ عملية تشفير البيانات ويصبح بعدها صاحب الجهاز غير قادر على الوصول إليها. آلاف الأجهزة العاملة بنظام التشغيل ويندوز تضررت من هذا الفايروس الذي اجتاح العالم في عام 2017 وضرب أكثر من 100 دولة. فاحرص بالاحتفاظ بنسخة احتياطية من ملفاتك باستمرار ودوريا، ولا تضغط مطلقا على أي رابط لا تثق به في صفحة ويب أو يصلك عبر فيس بوك أو تطبيقات التراسل مثل واتساب وغيرها من التطبيقات.

نصائح لإنشاء كلمة مرور قوية:

- يجب أن تحتوي على حروف كبيرة وصغيرة وأرقام ورموز مثال (#$&@%*).
- اجعلها مختلفة من حساب لآخر.
- يجب تغييرها بين الفترة والأخرى.
- ابتعد عن تواريخ الميلاد والأسماء الشخصية وأرقام الهواتف.
- يجب الحفاظ على سريتها وعدم الإفصاح عنها.
- لا تكتب أو تحفظ كلمة المرور على ورقة أو في رسالة البريد الإلكتروني.
- لا تستخدم خاصية تذكر كلمة المرور المتوافرة في بعض أنظمة التشغيل.

تجنب تنزيل المرفقات من البريد الإلكتروني مجهول المصدر

فعادة ما يلجأ المخترقون إلى إرسال ملفات مدمجة ببرمجيات خبيثة من خلال البريد الإلكتروني بهدف سرقة المعلومات الشخصية والسرية للضحية.

الخاتمة:

كتبت هذا الكتاب لتوسيع نطاق الوعي الأمني وتوعية المستخدمين بمخاطر الإنترنت، فثق تمامًا أن المعلومات التي ذكرتها صادقه، فيجب عليك أن تقف وتفكر قبل الإبحار في عالم الإنترنت، ويجب عليك أن تميز بين المفيد و المضر وبين الخطير والآمن،ولا تستهن بالإنترنت، واستشر ذوي الخبرة عند الوقوع في أبسط مشكلة، فالأمن كالسلسلة، تقاس قوتها بقوة أضعف حلقة فيها، واختراق البشر أصبح أسهل من اختراق الأجهزة، فاللعبة مكشوفة و الكرة في ملعبك.

الفهرس



السيرة الذاتية

المعلومات الشخصية:

- الاسم: سيف محمد الكعبي
- الجنسية: الإمارات
- تأريخ ومكان الميلاد: 1996-03-03 - العين
- الهاتف: 0501555914
- الحالة الاجتماعية: أعزب
- البريد الالكتروني: mr.kaabi-sp@hotmail.com

نبذة عامة:

- أنا طالب لديَّ طموح في الحياة. أدرس في كليات التقنية العليا بكالوريوس أمن المعلومات، لديَّ العديد من الأهداف في حياتي، ولا سيما تطوير نفسي في مجال أمن المعلومات، وهذا قادني إلى إعداد كتاب توعوي حول أمن المعلومات لتوجيه الناس ومنحهم لمحة عامة عن مزايا أمن المعلومات وعيوبها.

الخبرات:

- التدرب في شركة IBM في مجال الذكاء الاصطناعي بالتعاون مع شركة مبادلة.

التعليم:

- بكالوريوس أمن المعلومات - المؤسسة العليا للتكنولوجيا

الجوائز:

- الفوز بجائزة الشيخ زايد العالمية للبيئة - فئة الابتكار

الشهادات:

- شهادة في الاختراق الأخلاقي (معتمدة) من: Sensespot
- شهادة في الأمن الإلكتروني والاختراق الأخلاقي عبر الإنترنت (نظريًا) معتمدة من TeachCampus للتدريب التقني.
- شهادة "مقدمة إلى الشبكات" من CISCO Company.

المؤتمرات:

- المشاركة في مؤتمر الأمن السيبراتي في الشرق الأوسط.

الاهتمامات:

- القراءة
- الكتابة
- الحاسوب
- البرمجة

المهارات:

- الابتكار
- العمل الجماعي
- القيادة

اللغات:

- اللغة العربية (اللغة الأم)
- اللغة الانجليزية (جيد جدًا)

Skills

Innovation	Excellent
Teamwork	Excellent
Leadership	Excellent

Languages

Arabic	Mother Tongue
English	Very Good

Personal Info

Address

U.A,E

Al Ain

Phone

+971501555914

E-mail

mr.kaabi-sp@hotmail.com

Place of birth

Al Ain

Date of birth

1996-03-03

Marital status

Single

Nationality

U.A.E

hacking online (theoretically) from: cyber hacker certified. It is also accredited TeachCampus for technical training.

• The certificate of “introduction to networks” from CISCO Company.

Education

Unencrypted Information security – High Colleges of Technology

Additional Activities

Winner of Sheikh Zayed International Prize for the Environment -Innovation category

Participated in lectures on cyber security at Khalifa Bin Zayed Secondary School, Ibn Khaldun Primary School and Al Nakheel Kindergarten

Conferences

Participate in the conference of cyber security in the Middle East

Interests

Reading

Writing

Computing

Programing

CV



Name: Saif Mohammed al kaabi

Summary

I am a student that has an ambition on my life, I study in high colleges of technology 3rd year, Information security specialization. Also, I have many goals in my life, especially, to develop myself on information security. This leads me to write an awareness book about information security to guide people and give them an overview about information security advantages and disadvantages.

Experience

IBM & MUBADALA
Trained in IBM Company in artificial intelligence with cooperation of MUBADALA in U.A.E.

Certificates

A certificate in moral hacking (applied) from: Sensespot institute.
A certificate in electronic security and moral

index

Conclusion:

I've wrote this book to aware the community about the dangers of the internet. That's why you have to trust what I have said in it, as you also need to sit and think with yourself before entering the world of the internet. You have to distinguish between the good and the bad, and between the safe and dangerous, and don't underestimate the usage of the internet. Always ask specialists when facing even the smallest of problems, because the game is being played, and the ball is in your field.

Avoid downloading links from unknown sources on the email. Hackers tend to send files that are attached to viruses through email. They do that for the purpose of stealing information and hacking devices.

How to create a strong password?

1. Your password should contain capital and small letters, numbers, and symbols (#$@*&).
2. Use a different in all your social media apps.
3. Change your password from time to time.
4. Don’t write a password that contains something like your date of birth, phone number, and personal name.
5. Keep your password a secret and don’t share it with anyone.
6. Don’t write your password on a paper or a mail.
7. Don’t use the “remember your password” option in certain systems.

The "ransom ware" virus:

The ransom ware virus is one of the most dangerous viruses that could affect systems; this virus can control an entire system and decode it. The hackers do this for the purposes of getting money. The virus main targets are the systems of huge companies, ministries, governments, hospitals and universities. The hacking starts when a message or a link sent by unknown person request to upload a folder as an important or personal folder. Once the folder is uploaded on the computer or the cell phone the encryption of data starts and the owner of the device cannot reach to his information. Thousands of devices by Microsoft windows get harmed from this virus that invade the world at 2017 and strikes more than 100 countries. So make sure to have always a backup on your files, and don't ever press on any link that you don't trust of it on website or received by Facebook or social media applications like WhatsApp any other applications.

What are the "things" in the internet of things?

Everything, everything can be a part of the internet of things. Cloths, kitchen wear, cars, furniture, even animals! Anything that the processing unit can get attach to and connect to the internet is a part of the internet of things. For example, some cow farms started to connect cow's bodies to the internet so they can keep checking on their overall health and fertilization, and to also measure the hormones which they release in their bodies so they can predict the best time for milking them. That helps in making accurate decisions in the industrial field! This means that if there's an error in production, then there's an error in our life!

The “internet of things”:

There are a lot of areas that tried to accurately define the term “internet of things”, but there isn’t any area that owns or controls the internet of things, that’s why you won’t find any definition for this term. Simply, all the definitions can mean one thing about the internet of things by the next text:

“The internet of things is a developed form of the internet that contains all the things in our life related to the connection to the internet to send and receive data to do certain things in the network”.

You may don’t like this theoretical definition, and I do as will, but truly, the internet of things is the world that we live some of its sides today. Some of the things we use have become able to connect the internet, like watches, televisions, glasses, etc. but the idea is not about just what we live, but it’s in the “things” meant in the internet of things.

Jailbreak risks, plus programs, and other application that download out of the store or official websites, once you download these applications on your device you plot your phone to hacking and stealing of your personal information and it is include stealing images, videos, chats, number and folders and more without your knowledge.

Artificial intelligence:

Artificial intelligence is one of the most important branches of computer sciences that support information security. It has a very promising future, and it makes me happy to see a minister of artificial intelligence in my country. Artificial intelligence is the machines ability to mimic the human capacity of thinking and evaluating and learning from past experiences. In other words, machines will be able to understand human beings, and it will be highly beneficial for us. The best form of artificial intelligence is robots. It is predictable that robots will be able to do human tasks, and more importantly, artificial intelligence will be able to provide information security. Artificial intelligence is the gate towards a bright future.

There are a lot of dangers related to the jail-break, plus, programe, and applications from computer stores. As long as you installed these apps on your phone, you'll become a target of hacking. All your personal data, photos, massages will get hacked without even noticing it.

Privacy and safety:

Are the terms "privacy" and "safety" mean the same thing? Of course no. safety means that as a user, you have to feel safe in general, but safety in the field of networking means that you as a user should have secured and safe applications and devices. Privacy means that as a user, you should have your privacy while using applications and electronic devices, and that no one should use my personal stuff. While technology keeps moving forward, we can't control the way of letting people share our private materials or not, but we can control the type of information that we can share daily. There's a phrase that says: "if you want me to protect you, then I have to watch you" and another phrase which says: "why do you fear being watched if you stay away from making mistakes?" of course I don't agree with these to phrases completely, but there are some things that makes some sense in them. The two phrases should complete each other if they were used on an equal term, but in reality they have a negative relationship. If you wanted safety, then this will affect your privacy.

The “Five Eyes” countries:

The five eyes country “united states of America, united kingdom, Canada, Australia, and New Zealand” cooperate with each other in the field of spying and watching networks of other countries and their communications as will. This alliance is headquartered in the national security agency and the British communication center. I’ve twitted years ago about this alliance when the exposing of Edward Snoden were published! Can you imagine that all what we write, share, and search for in the internet are under the watch of the five eyes countries.

hacking were emails, personal photos, video and phone calls, voice calls to internet protocols, files transfers, and the details of social networking.

Edward Snowden:

How can I write about information security without mentioning Edward Snowden? Edward Snowden is like the hero in the information security show. He is an expert computer specialist from American origins, and a former intelligent services agent. This man is responsible of the exposing a lot of crime about agents who he describes them as immoral and the first reason for doing this was that their working didn't represent the constitution of the United States, and he thought that exposing their behavior is the right thing to do so he can show the world about the past of the national security agency, and he also exposed a lot of things related to the agency, which included an unauthorized watching practices, which he thought that they tend to look to users private data. He spent years collecting evidence related to their actions and then he had exposed them for good, and he had accused them with violating the laws of national security by hacking user's data. The information that they had been

When you allow programs to view (your accounts, camera, photos, and microphone) then you are get yourself hacked, thus your data will be leaked.

Bitcoin:

In 2009, a mysterious person started explaining researches on the internet talking about the e-currency, how it functions, and what are its conditions, but in a sophisticated way. He named this the currency the “bit coin”. After that, the world starts knowing about the bit coin and began trading and trusting it. Bit coin is an electronic currency that can be coded in order of usage.

One of the advantages of the bit coin is that it can be transferred between individuals without having a mediator in the transferring process. Hackers prefer using this currency when asking for a ransom. This currencies value can reach 27500 AED, as its value increases when people get interested in using it.

be reached through browsers, but we can reach it inside the deep internet. The deep internet comprises 94% of the total web.

The dark internet:

The dark internet is a set of websites and data that browsers can't reach directly, as it requires special tools and methods to reach it directly, like Torr network. The usage of the dark internet differs between a person and another, but being far from daily watching, it is considered a center for illegal procedures. It is the suitable place for all sorts of crimes, especially drug and weapons dealing. There are a lot of websites that sells drugs and weapons and dangerous materials that can cause wars and conflicts, and there are a lot of websites that teaches illegal hacking, selling sensitive or private codes, or even selling nationalities and passports, and other websites that sells falls documents. These websites are all illegal, as they use virtual currencies like the bit coin.

Have you ever heard of the deep internet or the dark internet and that the internet can be split into three categories:

1. The Surface internet
2. The Deep internet
3. The Dark internet

The Surface internet:

The Surface internet is the network that we use in everyday life like searching in Google and watching articles. These are the websites which you can reach through browsers. The virtual internet comprises only 4% of the total web.

The deep internet:

The deep internet is the biggest part of the internet as it represents the networks and websites the normal browsers can't reach it, but we can reach it directly through special methods like internal query. Those can be like emails, bank information, and Facebook massages. These are data that can't

What is the new law of information protection in Europe?

Recently we noticed that a lot of massages arrived on the email from global companies telling us that they updated the using terms! The reason for this is that the EU has made a new law to protect the privacy of users.

In the 25th of May 2018 this law was applied on all companies the deals with the user's data either they were in Europe (or outside Europe with total control of their personal information). The law does deal a lot with the safety of people's personal data, and to allow them to have full control over it. I really wish if we can find a law like that in all countries, not just in Europe.

- Phishing emails:
- It is known as fraud or trick someone (part of social engineering), for clarity, someone creates a website looks 100% as a commercial website.

Technology is a man-made thing, and humans are the essential beings in building them. Human mistakes are always possible to happen, but fixing them requires a lot of time and effort, and we should not forget that regular people tend to be soft and sensitive, and they're easy to fool. There's also some neglecting to this issue, either it was accidently or by ignoring, and technology keeps advancing rapidly, and that needs a lot of care.

What is the weakest link in any system?

Whatever the system is extremely safe and secured that doesn't mean that there are some weak points in it, because in the end there isn't a system that is a 100% secured. If we said that the system is secured perfectly, then what is the weakest point?

Humans, yes humans. The user is the weakest point in the system. Every cyber-attack that happens to the system depends on the human mistakes (pressing an untrusted link, opening a file that is full of viruses).

Reasons for getting viruses:

1. 46% phishing emails
2. 36% lacking of employees to be trained
3. 12% untrusted websites and adds
4. 1% a problem in the system
5. 5% other reasons

Information war:

The Second World War is not the last war in the history of humanity. There are wars that keep happening all the time in the world of the internet. These wars use sensitive information as a weapon; it can be on a wide scale and against information systems. It happens in the case of having the ability to it not in the need. Information war can include all types of strategic information, making sure of providing these information, and spreading propaganda or false information to break people mentally. Information war has become an essential part of military war. The head of the germen intelligence services August Huning said: “from now on, wars will become something related only to the internet, and soldiers will train on hacking devices and information, and every country does create viruses for the purpose of deceiving the enemy and immobilize their communication field”.

Providing someone with the necessary tools to secure himself from hacking will protect him for a short while, but teaching him about its way of working will secure him longer.

Encryption:

The technologies and politics of encryption have an exceptional attention today at the information security field. This lead to make the protection of encryption the most important way to reach the three functions of security, which are; confidentiality, integration and availability of information and service. Also, it is a main component for other security technologies and techniques, especially, in the electronic field, online trade, email, and generally the exchange data by electronic devices.

In terms of its concept, encryption pass through two main stages; the first is the text encryptions which convert the typing text to incomprehensible symbols. Second, decoding the encrypted text and return to a readable and understandable text, this equation done by encryption programs which have different types and functions.

that spread immediately when it access the device, and starts destroying which lead to inhibiting the level of internet connection service, which results a difficulty in reaching to services according to the huge amount of the received data in the device.

Spyware:

They are programs that can be downloaded secretly in the device to record all passwords and secret private massages and information.

The common between these programs that are a harmful programs that work for destruction even to destroy the system, programs, folders, functions or to perform illegal tasks such as making a scam or cheating in the system, and the truth is that it is not synonymous terms of common viruses, but it differ on each other according to its formation and sometimes upon the result of harm or it way of attack.

Programs that can harm information systems:

Computer viruses:

A type of program used in a wrong way to work with other programs or files.

Worms:

An independent type of a computer programs that can copy itself to other devices through the internet.

Trojan horse :

A program that looks like it's going to work in a certain way, but in fact, it works in a way that could damage the information.

Denial of Service Attacks:

It also known as hiding of service attacks, and it is an attack done by a hacker by supplying number of websites with a huge amount of unnecessary data, and it is carried by viruses

How can you protect your children from the internet?

Remember always that your awareness is the safety way for you and your children. You have to keep warning them about contacting with strangers and sharing their personal information with them whoever are they. Make sure to let them gain your trust smoothly when they want to share anything in the social media field, and try to follow the type of information that they share in social media, because it's full of strangers who always want to harm others, either by extortion or stealing information. Our children lack the necessary knowledge, that's why we have to keep warning them about information security.

One of the hacking methods is using text massages. It works through sending some false massages like: you have won with us, send us your bank account, sign your information, and a lot of different massages with the same tune. This method is used to hack through personal information.

Wars have become only trash-talk in the era of social media. If you opened a social media app you'll find all sort of news. You'll see people with all their differences attacking each other, even those who are from the same country! But why is that!? Aren't we supposed to be a united nation!? We in the United Arab Emirates have taught from our late father sheikh Zayed bin sultan that whatever happens between us, we are still one. It really breaks my heart to see someone insulting my country in the social media field, because when it comes to my country, it's a clear red line for me.

The "social media" chaos:

Our daily life doesn't move without social media that people use for their own benefits. Since that everyone who entered this field has become popular, and the idea became reversed. We know that the increasing of demanding's will increase the offer, but in the field of social media, it's vise-versa, and suddenly everyone becomes an enlightened person. For an example, if you entered a twitter account, you'll find someone writing about everything. This can be realized in any social media app.

These apps were designed for a lot of proposes, but it doesn't suit all users, that's why they had to put suitable goals for them. If you tried to criticize them you will get insulted, and even if you shared a material in which they don't like, you will get insulted as will. People didn't change so as life. What had truly changed are the principles and values. That's why the phrase "say well or stay silent" does no longer exist.

Why information security is important?

Information security is important with today's technological advance, since information technology has become reliable on doing every day's work and that computer have widely spread, and we should not forget that the developing of the information technology has increased greatly. That alone is dangerous, because we are not ready for this fast development, why? Because we don't possess the tools to protect our information, and there's no investments is this field! And because of this, the door is widely opened for hackers.

processing stages or exchanging stages even in the internal transaction with information or illegal interruption. For example, a generalization cannot be edited by anyone.

- **Availability of information and service**

  Ensure that the information system continues to work and able to interact with other information and serve other websites. Moreover, the user of this information will not be prevented of using the information or access to it. For example; the ability to access the system page of employees.

Information security:

Information security is a number of policies and laws that are taken to prohibit those who are not allowed to change the information, steal it, or to hack the entire system, but from my point of view, I think that information security is the process of keeping the information safe, and protect it from unauthorized people.

There are three main principles in information security:

- **Confidentiality**

  It means that you must be sure that the information cannot be appear or shown to any unauthorized person. For instance; a folder cannot be shown to any employee except the manager.

- **integration**

  Making sure that the content of information is correct and is not edited, especially, the content is not destroyed or changed or edited in any stage of

Can you imagine that hacking a camera takes only a fraction of a second? And you can be threatening all your life through this? So make sure to put a tape on your camera to avoid this.

Social Engineering:

Can you imagine that social engineering happens in the US every two minutes?

In the information security and digital security fields we can define Social engineering as the ability to acquire sensitive and secret information through manipulating the victim to gain his trust smoothly. Social engineering helps hackers to hack systems through manipulating people and machines as will. Social engineering is the simplest way of hacking since it comprises 70% of world hacking. Because it does not rely on knowing a deep technique, so anyone who has some intelligence, smartness or experience can do some hacking by using social engineering. To avoid to be a victim of these kind of hacking, you should take care of your privacy and do not share any personal information about yourself, because the hacker or the attacker can use it to impersonating you, so you should not trust anyone. Be careful and aware to every email or message that contain files or included links.

Why do we need Security Awareness?

The information security section in a company cannot withstand all the dangers and deal with is alone. Every employee in the company should have the responsibility towards the coming dangers. The lack of knowledge related to information security for a single employee could lead to disasters. That's why every employee should have the knowledge to be aware towards these dangers.

Targets of security awareness:

The main targets for knowing security awareness are people who work in companies and organizations and in the governments as well, because they can get to know the sensitive information that no one is allowed to know about except for them, and that depends on the position of the employee in the company and his need to the information.

What is “Security Awareness”?

Security awareness means that every individual should be holding the responsibility towards the information and devices that he uses, either it was personal or related to the working network, or it also includes his total realization of not talking about the passwords and information in the company, and also knowing the dangers related to these actions. That helps improving the sense of responsibility and understanding of the importance of following the security laws that are given from the authorities. Security awareness is considered one of the most important lines of defense because of its low cost. Studies have proved that the amount of money spent on the awareness of employees or people in general are far more less than the money spent on fixing the damages that are caused from hacking information.

Our daily life has become boring, and communication between people became only needed for material purposes. It's true that the internet made a lot of positive contributions, as communication between people is fast, and governmental institutions are becoming more active, as well as the resident, but in the future, all the disadvantages will increase, and we have to prepare for this, because the next war will be cyber.

Introduction:

I'm not an author, but I really love and feel jealous towards my country which taught me a lot, and helped me to achieve my goals. I started spreading awareness about the dangers of the internet through giving lectures, and I founded that our community needs more awareness about security, and that is the reason that moved me to write an awareness book for the community as a whole.

There's no doubt that information security has become one of the most fast growing sectors in this case, especially with the increasing of cyber-crimes. We keep hearing about crimes that happen to people who get hacked and their information's get leaked or they are robbed here and there, and that's what made different trading companies to give more priority for services related to information security, and countries should increase the awareness for the community so they can stay safe from cyber-crimes.

Cybersecurity is one of the most important disciplines and skills that have been increasing since 2005 until now and in the future due to the high use of technology and the increased opportunities and possibility of diversion and theft of data and violation of privacy for all users and devices such as mobile phones, smart TV, smart cars, intelligent home appliances to spread malware and electronic warfare against government agencies And companies, causing the loss of hundreds of millions of data and money. It is important to create national and Arab cadres and to develop plans to prevent and avoid cyber risks and to protect our privacy. In 2021, there will be 3.5 million cyber jobs. We need professionals and specialists in this field, but in the Middle East there is still weakness and lack of professionals and professionals in this. The field in practical application and weakness in the Arab sources to educate the Arab nation of young people, but such an Arab book and some Arab youth initiatives recently to raise the level of security culture is proud and certainly will be an honorable sign of the Arab and Islamic world in the field of cybersecurity.

Dr. Yasser Alosefer

Cyber Security Entrepreneur

I have seen Saif exploring sophisticated cyber security solution since I met him. He has been running several security awareness campaigns in the community, particularly for young students who are using smart devices for private use. The awareness campaigns are very helpful for the community to keep them protected against malicious attacks. The book is a must read for all and particularly for all users of smart phones who use them for private and enterprise .

Dr.Munir Navid

Assistant Professor - Computer and Information Science

Al Ain College of Students

Information security has become very significant in many organizations impacting them in different ways. In his book, Saif Alkaabi is raising important awareness of information security and the effect that it has in terms of privacy concerns and the challenges that security brings to our world today and the strong increase in information security threats. The book also increases understanding of the key concepts of information security and the benefits technologies bring to deal with the various challenges of information security.

Dr. Khalid Samara

Head of Department - Computer and Information Technology

Al Ain College of Students

(3145/7/2018)

Isbn 978-9957-99-882-0



Security Information unencrypted

Saif Mohammed Alkaabi

2018م



Security Information

unencrypted